Submitted September 24, 2017 by author: Amali De Silva-Mitchell, Futurist (United Kingdom / Sri-Lanka), Past Director Freedom of Information & Privacy Association of BC, Canada; Past President Vancouver Community Network, BC, Canada; UN WSIS-CS Sector Participant.

To: IGF BPF Cybersecurity List at bp_cybersec_2016@intgovforum.org

Re: 2017 BPF on Cybersecurity; Questions:

- *How does good cybersecurity contribute to the growth of and trust in ICTs and Internet Technologies, and their ability to support the Sustainable Development Goals (SDGs)?*

  Citizens come to rely on ICTs; Internet of Things IoT; and Artificial Intelligence AI; into the future for their daily activities. They don't see a future without it, when trust is good. As such, government and business service delivery and product development consider it their backbone, or highway (older concept) and enabler for efficient, cost effective outcomes. However, in full trust there is risk of over-reliance (over-trust), and there is perhaps a failure for good thought out contingency plans (ICT will never really, fail), that are not sufficient to meet unexpected events such as Acts of God such as earthquakes which can impact ICTs significantly, or even significant changes in government political policy, e.g. cutbacks to ICT maintenance due to a mass famine that has priority to be serviced.

- *How does poor cybersecurity hinder the growth of and trust in ICTs and Internet Technologies, and their ability to support the Sustainable Development Goals (SDGs)?*

  Development of the dark side of the internet, loss of public trust and accountability, development of public fear, poor service or product delivery which could also leading to lower investment in public private partnerships, ability to raise capital etc. Can result in messy, faulty internet of things IoT, that can lead even to serious physical impacts on citizens e.g. defective four-way road stop leading to driver accidents etc. Low productivity, general malaise and slow progress of SDG attainment may result Extreme frustration of policy makers leading to abandonment or over simplification of of goals, with no real substance with respect to effective outcomes. It can lead to simply a play on performance measurement indicator presentations.

- *Assessment of the CENB Phase II policy recommendations identified a few clear threats. Do you see particular policy options to help address, with particular attention to the multi-stakeholder environment, the following cybersecurity challenges:*

  1. *Denial of Service attacks and other cybersecurity issues that impact the reliability and access to Internet services:*
     Each country needs a designated site where the ISPs and others, including government can post outages, warnings, risks, etc. for the average user to access so as to protect themselves. The site must be easily accessible.
  2. *Security of mobile devices, which are the vehicle of Internet growth in many countries, and fulfill critical goals such as payments:*
     Good policies made available to citizens on managing their device. Low income citizens may have to be supported by the government for these private sector services.
  3. *Potential abuse by authorities, including surveillance of Internet usage, or the use of user-provided data for different purposes than intended*
     Ethics as mandated by government policy is key to a healthy economy. There has to be government sector ICT / IoT / AI ethics education.

4. *Confidentiality and availability of sensitive information, in particular in medical and health services*
   Each person's data is his own. Companies collecting data must notify the user if they are profiling users, providing accessible audit trails and algorithms. The manner and intent of big data analytics at an individual person level must be reported so that the user can opt out. Auto transfer or buying of a user's account by another company requires new consent from the user, including data transfer of the old profile of the user. Personal data collected is not the property of the company, it is the property of the individual and this must be respected. Important that jurisdictions in the third world, that do not have the rigorous standards for instance of the European Union, take action to equalize the fairness of these matters to other jurisdictions for their citizens, especially when dealing with foreign servicing companies. The foreign company can also be at risk regarding these matters retroactively with new legislation.
5. *Online abuse and gender-based violence*
6. *Security risks of shared critical services that support Internet access, such as the Domain Name System (DNS), and Internet Exchange Point (IXP) communities*
7. *Vulnerabilities in the technologies supporting industrial control systems*
   Ethical, inclusive, global, transparent use of protocols and standards to reduce risk. These standards are for public use and must not be copyrighted to an organization, and can hence be accessed with no charge, so that smaller developers can be expected to meet all required standards. A user complaint system or ombudsman must be set up and systematic times reviews and action taken by regulatory bodies. All risks must be openly identified to the user. A sort of FDA (Food & Drug Administration) approval system may also be suitable for new products and services
8. *Use of information collected for a particular purpose, being repurposed for other, inappropriate purposes. For instance, theft of information from smart meters, smart grids and Internet of Things devices for competitive reasons, or the de-anonymization of improperly anonymized citizen data*
   This is all about ethics and there should be an ethics oversight bureau that systematically audits all companies on the globe for compliance with data repurpose without user consent. This could be onerous for the user to consent to everything but perhaps the bureau can set up a profile that users keep up to date indicating their wavers and opt outs.
9. *The lack of Secure Development Processes combined with an immense growth in the technologies being created and used on a daily basis*
   Good standards and protocols, per country, per region, globally (for issues of cultural sensitivity) are mandatory including protocols for human-computer interaction.
10. *Unauthorized access to devices that take an increasing role in people's daily lives*
    Each government / jurisdiction has to set policy and standards of conduct and enforce it. A complaints system for the citizen must exist.
11. *Other: describe a cybersecurity issue critical to developing the SDGs in ways not listed above relevant to your stakeholder community (100 words or less)*
    Lack of education in these issues for the average citizen, especially in developing countries, with over trust of companies have "good" intentions at all times, is going to cause unhappiness that can lead to trust issues for the future. Governments must educate its populations through TV, radio, town hall meetings etc. These are the new manner of civilization and the protocols must be taught. Whistle blower legislation and implementation is key for good governance, but it should not be a witch-hunt procedure or used for malicious purposes, and hence requires administration with excellent judgement.

- *Many Internet developments do not happen in a highly coordinated way - a technology may be developed in the technical community or private sector, and used by other communities and interact in unexpected*

ways. Stakeholders are managing complexity.
This both shows the strength and opportunities of ICTs and Internet Technologies, but also the potential risks. New technologies may be insufficiently secure, resulting in harms when they are deployed: conversely, we may adopt security requirements or measures that prevent the development, deployment, or widespread use of technologies that would generate unforeseen benefits. Where do you think lies the responsibility of each stakeholder community in helping ensure cybersecurity does not hinder future Internet development?

Collaboration, communication, inclusiveness, transparency with honest ethics conducted in a timely, fair manner. Accountability, integrity and deep cultural understanding are important. IoT and AI are going to add a complexity that is going to require some sophistication to understand the issues, but it must be discussed at an educated layman's level to enable effective feedback from MAGs. Regular public / expert surveys can assist effective policy making e.g. found in action currently in the US, Canada, European Union etc. Examples of such work are: Pan-European dialogue on Internet governance (EuroDIG); The Pew Research Center's Internet & American Life Project, Work of the Privacy Commissioner of Canada; United Kingdom Governments Digital Strategy work etc. The average citizen must be surveyed as well as there must be a mechanism that any citizen or person can send in feedback to an independent body.

- *What is for you the most critical cybersecurity issue that needs solving and would benefit most from a multi-stakeholder approach within this BPF? Should any stakeholders be specifically invited in order for this issue to be addressed?*

Lack of education of the public at each age, income level, cultural grouping and educating the public on internet ethics and etiquette now commonly mentioned. Education of risks, preventative measures, safety online, derived issues, repercussions etc. must be communicated at a meaningful level for the average citizen. Just having it on-line does not mean the average person will look it up. Awareness has to be generated and an "engagement" with the public established so that citizens past the school age have access to the information. Delivery means reaching all citizens not just making it available.